What is claimed is:

1. A method for accessing cryptographic material comprising the steps of:

creating cryptographic material, by a first Cryptographic-related application programming interface ("API"), in response to a request by a first application compatible with the first Cryptographic-related API; and

creating a supplemental aspect of the cryptographic material by a supplemental method for the first cryptographic API, wherein the supplemental aspect includes information for rendering the cryptographic material compatible with a second Cryptographic-related API so that the cryptographic material is accessible for a second application by the second Cryptographic-related API.

2. The method of claim 1, wherein the step of creating cryptographic material comprises creating a certificate or private key, and the step of creating the supplemental aspect of the cryptographic material comprises the steps of:

deriving a key container name from the certificate or private key; and

determining whether the key container already exists.

3. The method of claim 2, wherein the step of deriving a key container name comprises the steps of:

creating a hash responsive to material from the certificate or private key; and

encoding the hash.

4. The method of claim 2, wherein the step of creating a certificate or private key comprises creating the private key and wherein if the key container already exists for the key, the step of creating the supplemental aspect of the cryptographic material comprises the steps of:

determining whether the key container contains a certificate;

associating the private key as a member of a key pair associated with the certificate, if the key container contains a certificate; and

associating the private key as a member of a key pair having a default key specification, if the key container does not contain a certificate.

5. The method of claim 2, wherein the step of creating a certificate or private key comprises creating the certificate, and the step of creating the supplemental aspect of the cryptographic material comprises the steps of:

extracting a key specification from the certificate; and

associating the certificate with a key pair under the extracted key specification.

6. The method of claim 2, wherein the step of creating a certificate or private key comprises creating the certificate, and wherein if the key container already exists for the certificate the step of creating the supplemental aspect of the cryptographic material comprises the steps of:

determining whether the key container has a private key; and

associating the private key with a same key pair as the certificate, if the key container has the private key.

7. The method of claim 2, wherein the step of creating a certificate or private key comprises creating the certificate, and the step of creating the supplemental aspect of the cryptographic material comprises the step of:

creating a public key from information in the certificate.

8. The method of claim 1, wherein the first Cryptographic-related API is one from the set of PKCS #11, CryptoAPI, and CDSA compatible API's, and the second Cryptographic-related API is not the same API as the first and is also one from the set of PKCS #11, CryptoAPI and CDSA compatible API's.

9. The method of claim 1, wherein the first Cryptographic-related API uses a certain term and the second Cryptographic-related API has a corresponding term, and wherein creating the supplemental aspect comprises creating material indicating a cross-reference between the terms.

10. A computer program product for accessing cryptographic material comprising:

first instructions for creating cryptographic material, by a first Cryptographic-related application programming interface ("API"), in response to a request by a first application compatible with the first Cryptographic-related API; and

second instructions for creating a supplemental aspect of the cryptographic material for the first cryptographic API, wherein the supplemental aspect includes information for rendering the cryptographic material compatible with a second Cryptographic-related API so the cryptographic material is accessible for a second application by the second Cryptographic-related API.

11. The computer program product of claim 10, wherein the first instructions comprise instructions for creating a certificate or private key, and the second instructions comprise:

instructions for deriving a key container name from the certificate or private key; and

instructions for determining whether the key container already exists.

12. The computer program product of claim 11, wherein the instructions for deriving a key container name comprise:

instructions for creating a hash responsive to material from the certificate or private key; and

instructions for encoding the hash.

13. The computer program product of claim 11, wherein the instructions for creating a certificate or private key comprise instructions for creating the private key, and the second instructions comprise:

instructions for determining whether the key container contains a certificate, if the key container does already exist for the key;

instructions for associating the private key as a member of a key pair associated with the certificate, if the key container contains a certificate; and

instructions for associating the private key as a member of a key pair having a default key specification, if the key container does not contain a certificate.

14. The computer program product of claim 11, wherein the instructions for creating a certificate or private key comprise instructions for creating the certificate, and the second instructions comprise:

instructions for extracting a key specification from the certificate; and

instructions for associating the certificate with a key pair under the extracted key specification.

15. The of claim 11, wherein the instructions for creating a certificate or private key comprise instructions for creating the certificate, and wherein the second instructions comprise:

determining whether the key container has a private key, if a key container does already exist for the certificate; and

associating the private key with a same key pair as the certificate, if the key container has the private key.

16. The computer program product of claim 11, wherein the instructions for creating a certificate or private key comprise instructions for creating the certificate, and wherein the second instructions comprise:

instructions for creating a public key from information in the certificate.

17. The computer program product of claim 10, wherein the first Cryptographic-related API is one from the set of PKCS #11, CryptoAPI, and CDSA compatible API's, and the second Cryptographic-related API is a different API than the first Cryptographic-related API and is also one from the set of PKCS #11, CryptoAPI and CDSA compatible API's.

18. The computer program product of claim 10, wherein the first Cryptographic-related API uses a certain term and the second Cryptographic-related API has a corresponding term, and wherein the instructions for creating the supplemental aspect comprise instructions for creating material indicating a cross-reference between the terms.

19. An apparatus for accessing cryptographic material comprising:

a processor; and

a memory coupled to the processor for storing instructions for controlling the processor, wherein the processor is operative with the instructions to perform the steps of:

a) creating cryptographic material, by a first Cryptographic-related application programming interface ("API"), in response to a request by a first application compatible with the first Cryptographic-related API; and

b) creating a supplemental aspect of the cryptographic material by a supplemental method for the first cryptographic API, wherein the supplemental aspect includes information for rendering the cryptographic material compatible with a second Cryptographic-related API so that the cryptographic material is accessible for a second application by the second Cryptographic-related API.

20. The apparatus of claim 19, wherein step a) comprises creating a certificate or private key, and step b) comprises the steps of:

deriving a key container name from the certificate or private key; and

determining whether the key container already exists.

21. The apparatus of claim 20, wherein the step of deriving a key container name comprises the steps of:

creating a hash responsive to material from the certificate or private key; and

encoding the hash.

22. The apparatus of claim 20, wherein the step of creating a certificate or private key comprises creating the private key and wherein if the key container already exists for the key, step b) comprises the steps of:

determining whether the key container contains a certificate;

associating the private key as a member of a key pair associated with the certificate, if the key container contains a certificate; and

associating the private key as a member of a key pair having a default key specification, if the key container does not contain a certificate.

23. The apparatus of claim 20, wherein the step of creating a certificate or private key comprises creating the certificate, and step b) comprises the steps of:

extracting a key specification from the certificate; and

associating the certificate with a key pair under the extracted key specification.

24. The apparatus of claim 20, wherein the step of creating a certificate or private key comprises creating the certificate, and wherein if the key container already exists for the certificate step b) comprises the steps of:

determining whether the key container has a private key; and

associating the private key with a same key pair as the certificate, if the key container has the private key.

25. The apparatus of claim 20, wherein the step of creating a certificate or private key comprises creating the certificate, and step b) comprises the step of:

creating a public key from information in the certificate.

26. The apparatus of claim 19, wherein the first Cryptographic-related API is one from the set of PKCS #11, CryptoAPI, and CDSA compatible API's, and the second Cryptographic-related API is not the same API as the first and is also one from the set of PKCS #11, CryptoAPI and CDSA compatible API's.

27. The apparatus of claim 19, wherein the first Cryptographic-related API uses a certain term and the second Cryptographic-related API has a corresponding term, and wherein creating the supplemental aspect comprises creating material indicating a cross-reference between the term